

DHS/FEMA Autumn Blend Demonstration

Northrop Grumman Credentials

November 15, 2010

Keith Ward

*Northrop Grumman Information Systems - SA&I
Director Enterprise Security & Identity Management
Transglobal Secure Collaboration Program (TSCP) Chairman*



Northrop Grumman

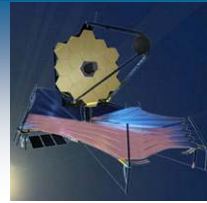
INFORMATION & SERVICES



ELECTRONICS



AEROSPACE



SHIPS



- **Designing** some of the world's most sophisticated war-fighting tools, from stealth fighters and airborne surveillance systems to nuclear powered aircraft carriers and submarines
- **Securing** the most sensitive systems and networks that are critical to our national defense
- **Establishing** interoperable trust mechanisms of our employees, our contractors, our suppliers, our customers' and our partners
 - **Trustworthy** and authorized to access systems and resources
 - **Proper due diligence** in checking their identities and backgrounds for the protection of sensitive information
 - **Timely notification** for de-provisioning identities from our systems and facilities



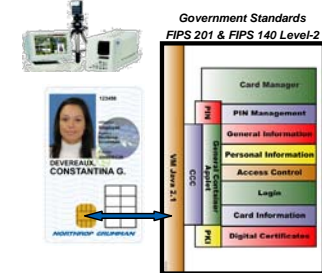
NGC's IDM PIV-I Approach – Current State

NORTHROP GRUMMAN

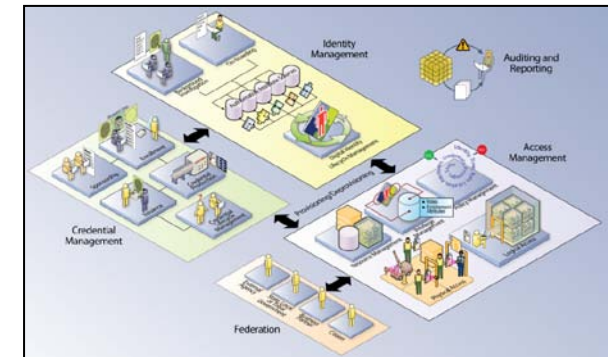
NGC Federated Common Identity Policy:

- **Smart Card & Electronics (GSA Certified)**
 - FIPS 201 (SP 800-85B) Electronics Testing
 - PIV 2 - Applets & Middleware
 - Auditor - OMB / Card & Electronics
- **FIPS 201 Process Lifecycle (ATO)**
 - Stakeholders, Process, Training (SP 800-79, 800-53/53A)
 - All FIPS 201 (GSA ABL) Compliant equipment
 - Auditor – Electrosoft (GSA's Agency Auditor)
- **CertiPath PKI (Certified)**
 - Cross certified to Federal Bridge
 - Bi-Lateral Trust with DOD (JITC)
 - Auditor – DoD's PKI Auditor
- **Key Recovery Practice Statement (KRPS) (Certified)**
 - Cross certified to Federal Bridge
 - Direct Bilateral Trust with DOD (JITC)
 - Auditor – DoD's PKI Auditor

Components & Infrastructure:



ICAM Architecture



IDM Solutions:

A single device that supports multiple authentication methods and enforces IDM policies across the enterprise

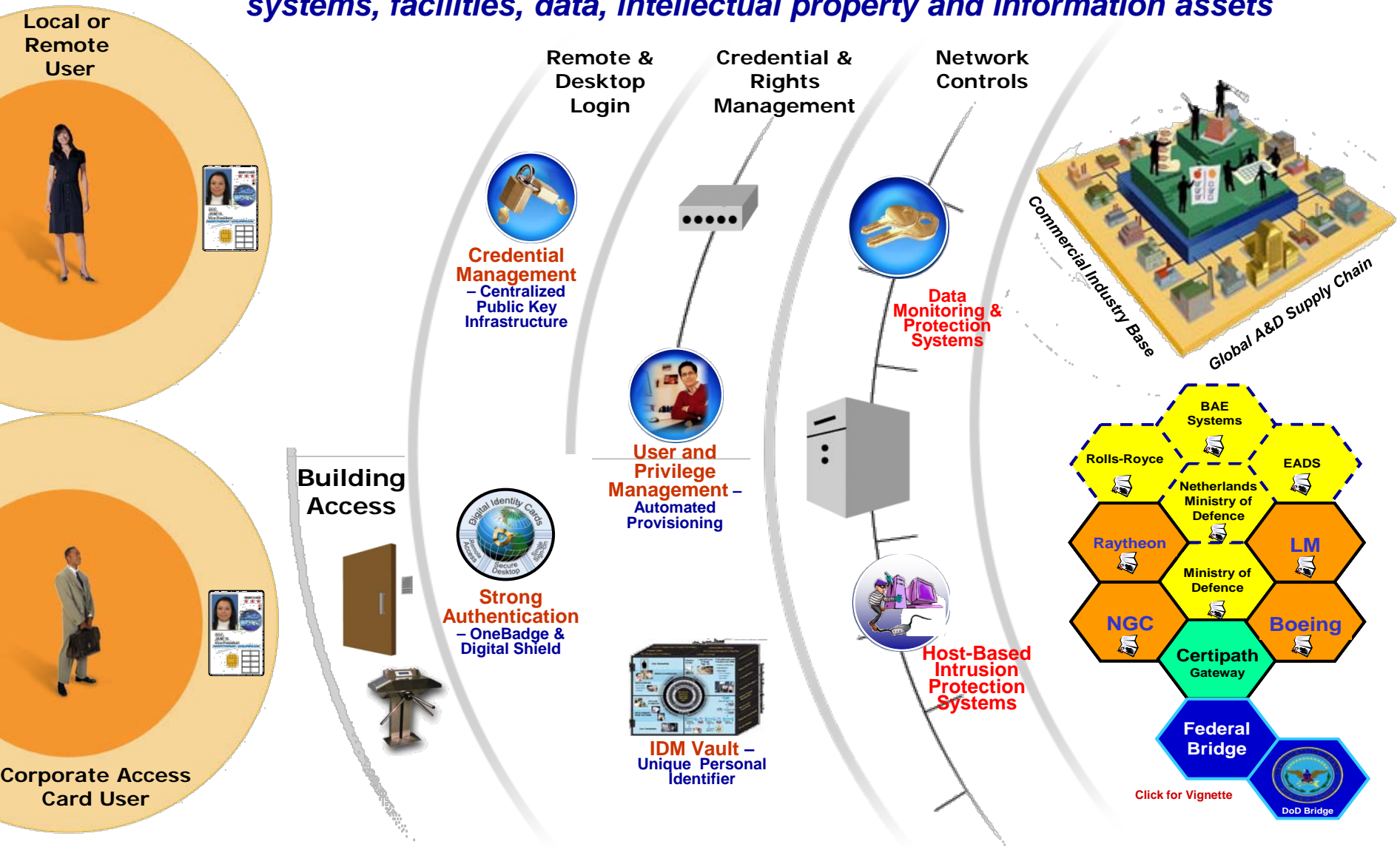
• Key Features

- Layered Technology Approach (When contract or security requires)
- One Time Password (Remote Access)
- Cross Certified CertiPath Certificate (Replacement of ECA Certificates)
- Desktop Middleware (2 or 3 factor Authentication)
- Single Sign-on (Password Vault)



Multi-Layer Security across the enterprise

Multi-Layered approach to provide additional security layers across our networks, systems, facilities, data, intellectual property and information assets



Autumn Blend Overview

Stakeholder Collaboration: FEMA Office of National Capital Region Coordination (NCRC), on behalf of the Personal Identity Verification-Interoperability (PIV-I)/First Responder Authentication Credential (FRAC) Technology Transition Work Group (TTWG), consisting of Federal, State, and Local membership stakeholders nationwide, is coordinating another FIPS 201 identity and attribute use case demonstration.

Trusted Technology Insertion: The Autumn Blend demonstration will occur on September 29, 2010, in Washington, D.C., and other TTWG jurisdictions nationwide. This is a demonstration of real credentialing interoperability for access management decisions, situational awareness, and post-event reconstruction. The active participants are “real” Federal, inter-State, and intra-State emergency response/recovery officials (F/EROs) and contingency personnel, as designated by their respective source authorities, who are subject to deploy for rescue or recovery missions.

All Hazards Risk Management: Autumn Blend integrates sponsored and registered F/EROs as defined in National doctrine, proven cyber-secure capability, and best practice solutions for “all hazards” risk mitigation. National doctrine includes the National Response Framework (NRF) for emergency support function (ESF) personnel, National Incident Management System (NIMS) for skilled inter-State deployers, National Infrastructure Protection Plan (NIPP) for Critical Infrastructure/Key Resources (CIKR) business continuity personnel, and National Continuity Policy Implementation Plan (NCPIP) for contingency personnel.



For Official Use Only (FOUO)





KANAWHA COUNTY
POLICE | FIRE | EMS

octo
DC OFFICE OF THE CHIEF TECHNOLOGY OFFICER

VAEmergency.com
Virginia Department of Emergency Management

NORTHROP GRUMMAN

PEMA
pennsylvania
EMERGENCY MANAGEMENT AGENCY

STRAC.ORG



FEMA



Participating Agencies / Jurisdictions

Active / EOC Participants

Federal

- DoD Buckley AFB
- DoD Pentagon Force Protection Agency (PFPA)
- Federal Emergency Management Agency (FEMA)
- Federal Aviation Administration (FAA)
- Transportation Security Administration (TSA)
- National Security Agency (NSA)
- Veterans Affairs

State and Local

- Cecil County, MD
- Colorado (CO)
- Hawaii
 - City and County of Honolulu
- Pennsylvania (PA)
 - Chester County, PA / Southeastern PA Regional Task Force
- Rhode Island (RI)
- Southwest Texas Regional Advisory Council for Trauma (STRAC)
- Virginia (VA)

CIKR

- Northrop Grumman

EOC Participants

- District of Columbia (DC)
- Missouri (MO)
- Pennsylvania (PA)
 - Pittsburgh
 - Pennsylvania Emergency Management Agency (PEMA)
 - Regional Logistics ProgramNY-NJ-CT-PA Combined Statistical Area
 - West Virginia (WV)
- Berkeley County, WV
- Jefferson County, WV
- Mineral County, WV
- Kanawha County, WV
- Raleigh County, WV

Fusion Center Participants

- CO
- WV



CAC / PIV / PIV-I Interoperability

CAC / PIV / PIV-I Credential Sponsorship & Issuance Process

Agency Management System with Personally Identifiable Information (PII)



Step 1

F/ERO eAttribute Sponsorship & Registration Process

F/ERO Repository with no PII
(contains public identities with numeric F/ERO attributes)



Step 2

Public Identity List (IL)

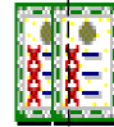


Step 2



Step 3

Public Identity and Privilege List (IPL)



"web-secure mailbox"



Management Station https secure internet connection auto feed

Relying Party eValidation Process

Jurisdiction-owned Management Stations and Validation Devices (validates and captures public transaction data)



Handheld Devices



Police Cruisers

Guard Station



CAC / PIV / PIV-I eValidation Process

Federal



SLTT



CIKR



Volunteers



Standard enables process to include:

1. D S C A
2. Mutual aid agreement
3. Business continuity agreements

Paper-based, visual or FIPS 201 eValidation to include:

1. ID (2 forms if visual)
2. Attribute or Affiliation
3. Deployment Source Authority



JRSOI



JRSOI = Joint Receiving Staging Operations Integration

Contingency Relocation or Response / Recovery Locations



Provides a real-time roster

Access Data:

- accountability
- traceability
- liability



Source	Location	Unit	Service	Phone
1. JRSOI - JRSOI	1. JRSOI	1. JRSOI	1. JRSOI	1. JRSOI
2. JRSOI - JRSOI	2. JRSOI	2. JRSOI	2. JRSOI	2. JRSOI
3. JRSOI - JRSOI	3. JRSOI	3. JRSOI	3. JRSOI	3. JRSOI
4. JRSOI - JRSOI	4. JRSOI	4. JRSOI	4. JRSOI	4. JRSOI
5. JRSOI - JRSOI	5. JRSOI	5. JRSOI	5. JRSOI	5. JRSOI
6. JRSOI - JRSOI	6. JRSOI	6. JRSOI	6. JRSOI	6. JRSOI
7. JRSOI - JRSOI	7. JRSOI	7. JRSOI	7. JRSOI	7. JRSOI
8. JRSOI - JRSOI	8. JRSOI	8. JRSOI	8. JRSOI	8. JRSOI
9. JRSOI - JRSOI	9. JRSOI	9. JRSOI	9. JRSOI	9. JRSOI
10. JRSOI - JRSOI	10. JRSOI	10. JRSOI	10. JRSOI	10. JRSOI

Sample Data Sheet

EOC

Geospatial
Human
Situational
Awareness
Display



FEMA

Achieving NIMS Credentialing Guideline Interoperability



Fusion Center / Emergency Operations Center (EOC) Geospatial Display

Date: September 29, 2010

Event: Fusion Center / Emergency Operations Centers (EOC) geospatial display of all stakeholder F/EROs nationwide who were electronically validated and permitted access to their respective locations for on-site accountability , resource situational awareness (liability) and post-event reconstruction (traceability)

Geospatial provider: Virginia Department of Emergency Management (VDEM), Virginia Interoperability Picture for Emergency Response (VIPER) geospatial application


EOC Agencies/Jurisdictions:

Federal: FEMA, DoD Buckley AFB, DoD Pentagon Force Pentagon Agency (PFPA), National Continuity Program (NCP), Transportation Security Administration (TSA)


SLTT/ CIKR: CO, HI, MD, MO, Regional Logistics Program (NY-NJ-CT-PA Combined Statistical Area), PA, RI, STRAC, VA, Berkeley County, WV; Chester County, PA/Southeastern PA Regional Task Force; Jefferson County, WV; Raleigh County, WV, Kanawha County , WV, Mineral County, WV, Northrop Grumman,

Fusion Center Jurisdictions:

State: CO, WV



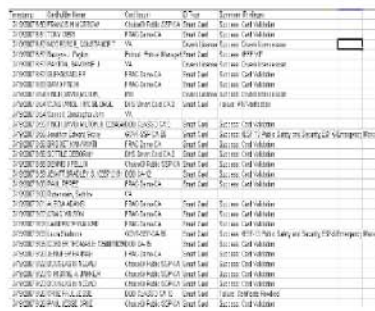
- Federal
- State and Local
- Critical Infrastructure / Key Resources



Provides a real-time roster

Access Data:

- accountability
- traceability
- liability



Sample Data Sheet

EOC



Scenario 1C: Mutual Aid Support (and reciprocity) Private to Public

Northrop Grumman / Virginia : NGC Newport Collaborative Effort

- Potential Participants and CAC / PIV / PIV-I Interoperability
 - Northrop Grumman PIV-I High Assurance
 - City of Newport News FRAC or NGC PIV-I Medium Assurance
 - VA State Police FRAC High Assurance
 - DoD Navy CAC High Assurance
 - Federal DHS PIV High Assurance
 - Targeted Capabilities List (TCL)
 - TCL 20 - Explosive Device Response Operations
 - TCL 28 - Onsite Incident Management
 - TCL 29 - Emergency Public Safety and Security Response
 - ESF 4 – Firefighting
 - ESF 5 – Emergency Management
 - ESF 13 - Public Safety and Security
 - CAC / PIV / PIV-I Authentication Business Rules:
 - 3-factor: 2-factor plus credential validation of digital photo on integrated circuit chip (ICC)
 - 4-factor: 3-factor plus credential validation of biometric on ICC
 - Authentication Technology and Software
 - PIVMAN
 - Partner and Newport News Physical Access control technology
 - Logical Access – TSCP Secure Email
 - Virginia's Interoperability Picture for Emergency Response (VIPER) Software
 - Authentication Technology and Software
 - Northrop Grumman Emergency Operation Center
- Date: September 29, 2010
 - Agencies/Jurisdictions:
 - Chester County, PA/Southeastern PA Regional Task Force (SEPA RTF); Northrop Grumman (NG) and Newport News (NN), Virginia (VA)
 - Targeted Population:
 - ESF 1, 4, 5, 10, 13
 - Sector 4, 6, 7, 8
 - Credentials:
 - CAC, PIV, and PIV-I



FEMA



What did we showcase

- The exercise showcased the ability to deploy a common, interoperable credentialing system that enables electronic identity authentication for government and industry personnel.
- The exercise succeeded in coordinating PIV credentials from emergency personnel representing state, local and federal agencies
- The NGC system worked across multiple domains and authentication infrastructures to deliver access management, situational awareness, cyber-secure communications and post-event reconstruction
- Participants in the exercise were validated electronically for physical access using mobile and fixed devices that verified identities through personal identification credentials, personal identification number and biometrics; and cleared for logical access through personal identification credentials that gave them computer access for secure email collaboration (TSCP Secure Email)

National Strategy for Trusted Identities in Cyberspace (NSTIC)



National Strategy for Trusted Identities in Cyberspace (NSTIC) & Transglobal Secure Collaboration Program (TSCP)



June 28, 2010

Information Assurance and Secure Collaboration "Illustrative" Technical Approach (Secure Email Collaboration)

Strategic Goals

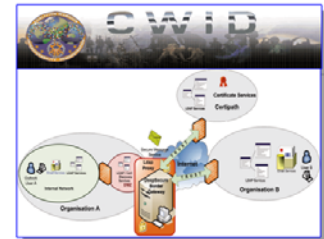
- **NSTIC GOAL 1:** Develop a comprehensive identity ecosystem framework
- **TSCP GOAL 1:** Enable secure information sharing within and between industry and governments

Business Case

- **Advanced Persistent Threat:** Government and community problem to mitigate exposure of enterprise Cyber Threats and comply with new regulations
- **Authentication:** Strengthening authentication across the enterprise with IDM Solutions
- **Improved Confidentiality:** E-mail is encrypted using medium assurance credentials

Sample Use Case Scenarios Include:

- ✓ **Use Case 1:** Test encrypted email between "Systems"
- ✓ **Use Case 2:** Test encrypted email between "Systems" with allowed attachment – Exchange APT Threat information in DIB
- ✓ **Use Case 3:** Exchange CUI data between partners using TSCP Secure Email Specification
- ✓ **Use Case 4:** Encrypted email using visual markers to help cultural aspects of security



Secure information sharing for collaboration between large commercial organizations and governments that assures the data is controlled and validated before release and provides assurance that organizational security policy is applied to data between internal security domains and at the boundary of an organization

12

NSTIC AND TSCP PLANNING MEETING



Identity Federation Services "Illustrative" Proposed Production Pilot

Strategic Goals

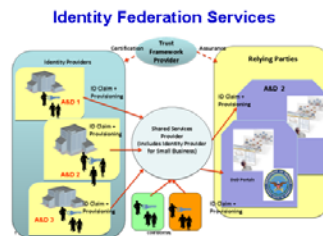
- **NSTIC GOALS 1, 2 & 3:**
 - Develop a comprehensive Identity Ecosystem Framework
 - Build and implement an interoperable identity infrastructure aligned with the Identity Ecosystem Framework
 - Enhance confidence and willingness to participate in the Identity Ecosystem
- **TSCP GOAL 1 & 3:**
 - Enable secure information sharing within and between industry and governments
 - Define interoperable specifications and solutions that enable re-use in a cost-effective manner across multiple programs

Business Case

- **Federated Common Identity Policy:** Employers vouch for employees identity attributes – Relying parties do not have to issue credentials and account provisioning is automated (cost reduction)
- **Advanced Persistent Threat:** Employees are using trusted computers and trusted networks to access CUI
- **Cost Control and Recovery:** Promote re-usable deployment of solutions to expedite implementation (decrease time to setup)

Sample Use Case Scenarios Include:

- ✓ **Use Case 1:** Company 1 employee logs into Company 1's network using company's issued Smart Badge (Windows Smart Card Login), that is compliant with Medium Hardware policies (re-use)
- ✓ **Use Case 2:** Company 1 employee accesses Company 2's application via the web. Company 1 passes the employee attributes such as Level of Assurance, employee status to Company 2 (Company 2 makes authorization decisions)



TSCP defined 'Common Operating Rules' that enable the Trust Framework, which is used by Relying Parties to make authorization decisions based on identity attributes from trusted Identity Providers

13

NSTIC AND TSCP PLANNING MEETING



Information Assurance and Secure Collaboration - Keith Ward "Illustrative" Full Scale Federated Exercise

Strategic Goals

- **NSTIC GOALS 1, 2 & 3:**
 - Develop a comprehensive Identity Ecosystem Framework
 - Build and implement an interoperable identity infrastructure aligned with the Identity Ecosystem Framework
 - Enhance confidence and willingness to participate in the Identity Ecosystem
- **TSCP GOAL 1 & 3:**
 - Enable secure information sharing within and between industry and governments
 - Define interoperable specifications and solutions that enable re-use in a cost-effective manner across multiple programs

Business Case

- **Federated Common Identity Policy:** TSCP Policies and Specifications align with DOD and Federal Identity Policies
- **Multi-Factor Security:** Multi-Factor approach to provide additional security layers across our networks, systems, facilities, data, intellectual property and information assets
- **Cost Control and Recovery:** Enterprise cost savings through enterprise deployment of TSCP Specifications while at the same time recover the cost of our investments

Sample Use Case Scenarios Include:

- ✓ **Use Case 1:** Identity interoperability (federation) of multi-level identity authentication across government & company domains
- ✓ **Use Case 2:** Identity Authentication at emergency venues to positively and securely authenticate authorized users for logical & physical access
- ✓ **Use Case 3:** Employees of critical businesses who work and/or reside in the impacted areas
- ✓ **Use Case 4-6:** Disaster Recovery, Pandemic & Cyber Threats Exercise



Potential Partners include:

- ✓ TSCP member Companies
- ✓ Department of Homeland Security
- ✓ FEMA
- ✓ State of Virginia (Governors Office)
- ✓ City of Newport News (VA)
- ✓ City of Hampton Roads (VA)
- ✓ District of Columbia - Metro
- ✓ State of Illinois
- ✓ City of Chicago
- ✓ Port of Chicago
- ✓ O'Hare Airport
- ✓ N.Y. Port Authority

14

NSTIC AND TSCP PLANNING MEETING



What can we coordinate to achieve success?

Implementation Pilots to demonstrate National Goals & Objectives.

- Identify the Gaps in existing national and agency policies
- Demonstrate Innovation
- Table Top and/or Production of PIV & PIV-I Interoperability

1. Leverage existing Government and Industry investments to date

- Existing global trust framework
- CertiPath Bridge
- Government and A&D issued credentials
- Commercial infrastructure investments

2. Demonstrate Level 3 & 4 Authentication (PIV, PIV-I)

- Business-to-Business
- Business-to-Government
- Government-to-Government
- Citizen-to-Business-to-Government

What can we coordinate to achieve success? (Demonstrations)

3. “Scale” - Recommendations and Feedback “GAPS”

- National & International Scale (global supply-chain)
- Regional, State and Local
 - Critical Infrastructure verticals; Healthcare, Financial, Energy
- Citizen’s using PIV-I credentials
 - Illustrative examples:
 - » I’m a Defense contractor who has a PIV-I credential but as a citizen I’m part of the community as a First Responder or a family member of an activated National Guard/Army Reservist.
 - » I’m a citizen accessing my Bank account information
 - » I’m a citizen using PIV-I credentials through Global Entry
 - » I’m a Fireman who needs access to CUI building information

4. PIV-I across international boundaries for adoption

- What are the Policy rules?
- What are the Technology challenges?
- What are the Privacy issues?
- What are the European issues and concerns?

Next Steps: Information Assurance and Secure Collaboration

“Illustrative” Full Scale Federated Exercise

• Strategic Goals

• **NSTIC GOALS 1, 2 & 3:**

- Develop a comprehensive Identity Ecosystem Framework
- Build and implement an interoperable identity infrastructure aligned with the Identity Ecosystem Framework
- Enhance confidence and willingness to participate in the Identity Ecosystem

• **TSCP GOAL 1 & 3:**

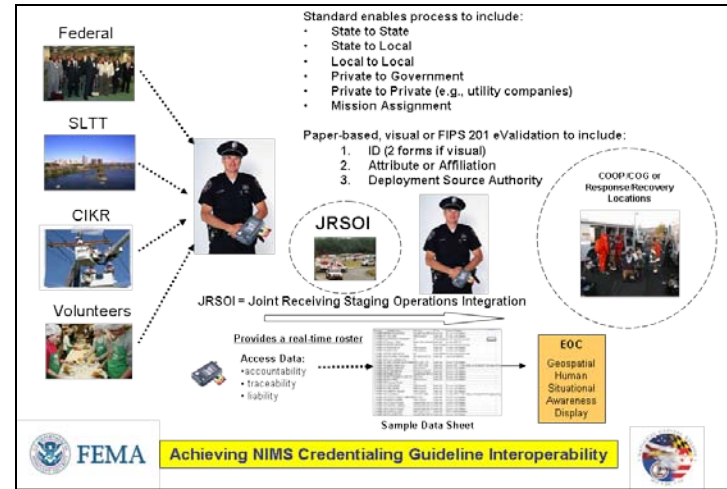
- Enable secure information sharing within and between industry and governments
- Define interoperable specifications and solutions that enable re-use in a cost-effective manner across multiple programs

• Business Case

- **Federated Common Identity Policy:** TSCP Policies and Specifications align with DOD and Federal Identity Policies
- **Multi-Factor Security:** Multi-Factor approach to provide additional security layers across our networks, systems, facilities, data, intellectual property and information assets
- **Cost Control and Recovery:** Enterprise cost savings through enterprise deployment of TSCP Specifications while at the same time recover the cost of our investments

• Sample Use Case Scenarios Include:

- ✓ **Use Case 1:** Identity interoperability (federation) of multi-level identity authentication across government & company domains
- ✓ **Use Case 2:** Identity Authentication at emergency venues to positively and securely authenticate authorized users for logical & physical access
- ✓ **Use Case 3:** Employees of critical businesses who work and/or reside in the impacted areas
- ✓ **Use Case 4-6:** Disaster Recovery, Pandemic & Cyber Threats Exercise



Potential Partners include:

- ✓ TSCP member Companies
- ✓ DOD
- ✓ Department of Homeland Security
- ✓ FEMA
- ✓ State of Virginia (Governors Office)
- ✓ City of Newport News (VA)
- ✓ City Hampton Roads (VA)
- ✓ District of Columbia - Metro
- ✓ State of Illinois
- ✓ City of Chicago
- ✓ Port of Chicago, O'Hare Airport
- ✓ N.Y. Port Authority

Transglobal Secure Collaboration Program (TSCP)

- Government-industry partnership specifically focused on **mitigating the risks related to compliance, complexity, cost and IT that are inherent in large-scale, collaborative programs that span national jurisdictions.**
- To do business in the world today, A&D companies must balance **the need to protect intellectual property (IP)** while demonstrating willingness and ability to meet contractual requirements from government customers for auditable, identity-based, secure flows of information.



Common Framework for Federated Collaboration

- **Identity Management & Information Assurance:**
 - Provide assurance that collaborative partners can be trusted
 - Meet government agencies' emerging requirements for identity assurance across domains
 - Establish common credentialing standards that accommodate and span national jurisdictions
 - Protect personal privacy data of employees
- **Data Protection:**
 - Define fine grain access right attributes for data labeling and data right's management
 - Establish "Application Awareness"
 - Demonstrate compliance with export control regulations
 - Protect corporate IP in collaborative and other information sharing programs
- **Facilitate Secure Collaboration:**
 - Provide collaborative toolsets that will interoperate with customers and suppliers
 - Facilitate re-use collaborative capabilities among multiple programs



NORTHROP GRUMMAN



Contact:

Keith Ward

Email: k.ward@ngc.com